

Department of Homeland Security's Protective Security Division

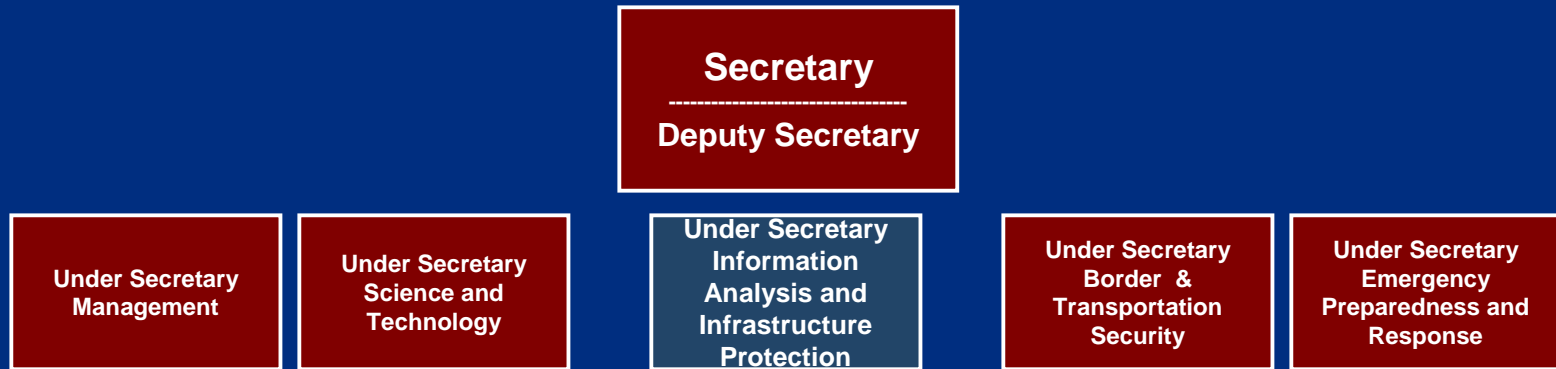
Lawrence M. Stanton, CPP

Chemical Industry Conference – Drug Enforcement Agency
September 14, 2004



Homeland
Security

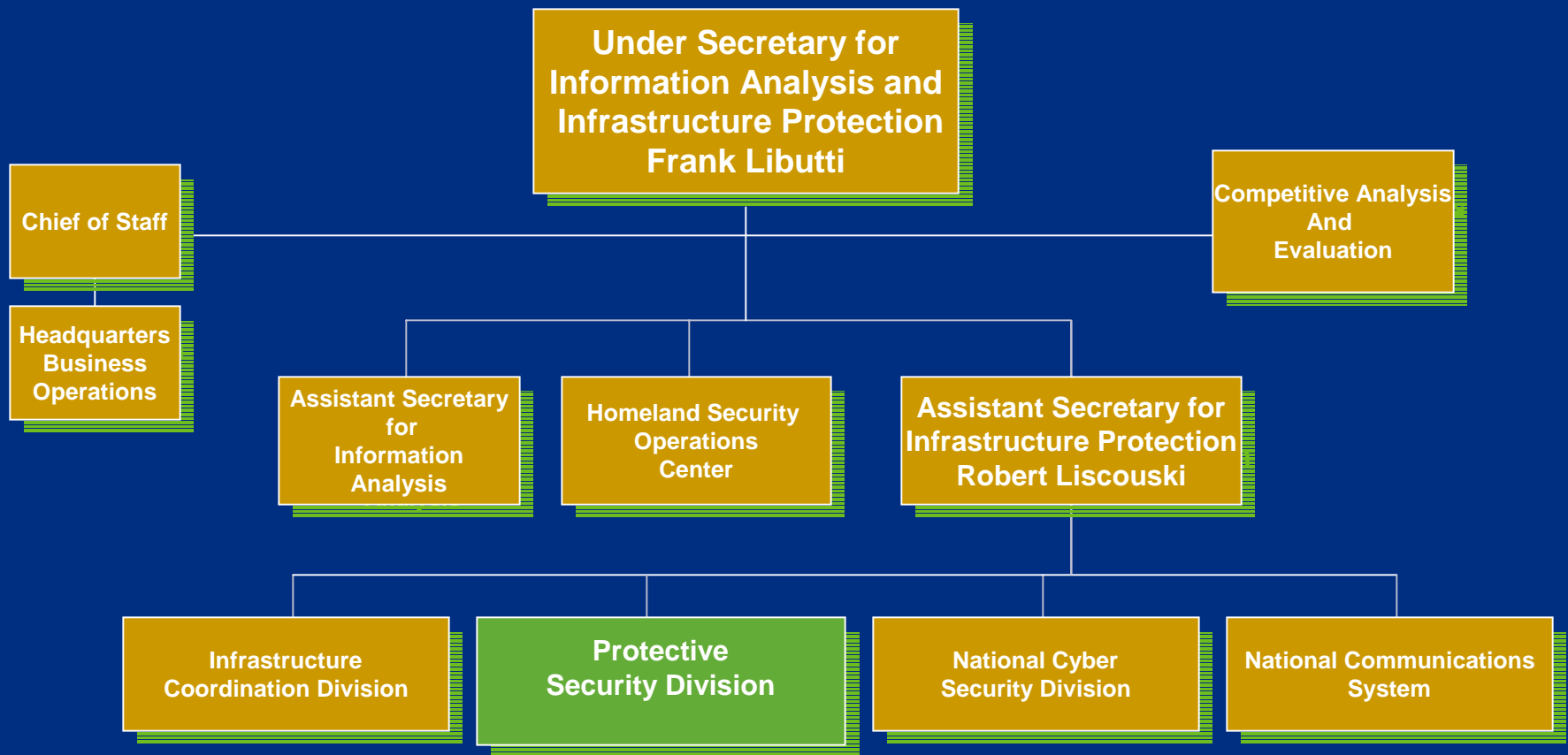
DHS Organization



**Homeland
Security**

FOR OFFICIAL USE ONLY

Information Analysis and Infrastructure Protection



**Homeland
Security**

FOR OFFICIAL USE ONLY

Who is doing what...

- What DHS is doing around you
- What DHS can and will do for/with you
- What you can do for DHS and the Nation



**Homeland
Security**

FOR OFFICIAL USE ONLY

National Infrastructure Protection Plan

- The NIPP is the baseline reference for DHS' efforts relative to the Nation's Critical Infrastructure
- Each Sector has a "Sector Specific Plan", an SSP, which
 - Describes the basic approach to securing the infrastructure
 - Assigns primary and supporting responsibilities
- Each Sector has a Sector Specific Agency, responsible for managing the security effort of the Sector
- DHS/PSD is the Sector Specific Agency for Chemical



Chemical Sector

- Focus of Main Effort to date has been sites with the capacity for high *Human Impact*
- Public number of “360” most dangerous facilities
- PSD has been working to apply reasonable metrics to the existing database in order to improve the quality of our priority list
- Next step – expand the definition of “Critical”
 - Economic Criticality – Place in the overall value chain
 - Psychological Criticality – Place in the Nation’s consciousness
 - Mission Criticality – Place in the Military, Public Health or Governance Structure



Major Activities

- Site Assistance Visits
- Buffer zone Protection Plans
- Sector Coordination Committees
- ISACs
- RAMCAP – other Analytical and Benchmarking tools
- Industry Best Practices
- All Aimed At...



**Homeland
Security**

FOR OFFICIAL USE ONLY

Partnership

- We need to build a Public/Private partnership in order to succeed
- We have looked closely at the example set by DEA, and we would like to emulate that relationship in several key ways:
 - Include associations and companies in the development... not only of a finished product, such as a program, a tool or something, but in the development of ideas and strategy.
 - Listen to the industry, keeping in mind that they are the experts, not us.
 - Remember the golden rule – First, Do No Harm



Site Assistance Visit

- **Coordination with State, Local and Facility**
- **Team threat briefing prior to a visit**
- **Vulnerability identification**
 - Vulnerability assessment review
 - Review existing vulnerability assessment(s) (if available)
 - If no VA exists, conduct joint vulnerability survey
 - Look for common infrastructure vulnerabilities
 - Discuss potential indicators of terrorism
 - Consider joint (industry/government) potential mitigation measures
- **Potential Government Assistance**
 - What protective measure suggestions does site have?
 - What additional government coordination is needed?
 - What DHS support is required?
 - What can DHS do to help your facility?



Buffer Zone Protection Plan

- Focus on both on-site and off-site (buffer zone) assistance
- Develop an improved understanding of:
 - Physical vulnerability to terrorist attack
 - Systems connectivity and interdependencies
- Identify problems and desired help in responding to elevated national security threat levels
- Broaden awareness and stimulate action to mitigate significant problems and improve preparedness (on-site and off-site)



USE ONLY



**Homeland
Security**

Communications Tools

- Chemical Sector Coordinating Committee
- Chemical Sector ISAC
- Analytical Tools – RAMCAP
- Benchmarking Studies
- Best Practices – Hopefully, a DHS version of the Chemical Handler's Manual



Other PSD Products and Services

- Information Sharing

Distribution of guides on Potential Indicators of Terrorist Activities, Common Characteristics and Vulnerabilities (for all asset types), best practices, and warning bulletins

- Security Standards

For vulnerability assessments and protective measures

- Technical Training

Terrorism awareness efforts, drills, exercises, and technical training

- Decision Support Tools

Sector security vulnerability methodologies; risk analysis methodologies; strategic and tactical analyses and assessments

- Modeling, Simulation, and Analysis

Development and utilization of advanced modeling and simulation capabilities to better understand and protect the Nation's complex infrastructure systems in concert with state and local governments and the private sector



**Homeland
Security**

FOR OFFICIAL USE ONLY

Outreach

- Engagement with industry and trade associations, i.e., speaking engagements at national conventions, videoconferences
- Interaction on selective basis with CEOs
- Availability of *Characteristics and Common Vulnerability* and *Potential Indicator of Terrorist Activity* reports
- Focused workshops, tabletop exercises and strategy games for clusters of high-risk activities (i.e., hazmat transportation, IT/telecom/cyber)
- Infrastructure Coordination Division and Office of Private Sector Liaison to serve as primary conduits



For your Part...

- Counter-diversion
- Counter-tampering
- Physical Security
- Cyber Security
- Participation



**Homeland
Security**

FOR OFFICIAL USE ONLY

Counter-diversion

- Threat stream information continues to indicate ties between narco-cartels and Al-Qaida
- There is little question that both information/intelligence and money is flowing between the two elements
- This raises two important issues for the fine chemicals and pharmaceutical industries:
 1. The exchange of information between these groups will inevitably **RAISE THE PROFILE** of your industry and individual companies
 2. The flow of money between these groups puts you in position to have a **REAL IMPACT** on the ability of Al-Qaida to harm us

Extending a best practice

- This industry has developed the “best practice” for preventing theft and diversion
- Those practices now need to be extended to:
 - Weapons precursor chemicals
 - Simple/Safe chemistry HE precursors
- And your insight is needed in developing new “Best Practices”



Other Practices

- Counter-Tampering, Counter-sabotage
- Physical Security
- Cyber Security
- And especially – counter-surveillance
- All this amounts to Participation



**Homeland
Security**

FOR OFFICIAL USE ONLY

Contacts

Larry Stanton

Protective Security Division

IAIP, Department of Homeland
Security

202 – 282 – 8371

lawrence.stanton@dhs.gov

Cheryl Coto

Protective Security Division

IAIP, Department of Homeland
Security

202 – 282 – 8734

cheryl.coto@dhs.gov



Bio – Larry Stanton

Larry is both a Certified Protection Professional (CPP) and a certified Fraud Examiner (CFE). He served as a commissioned officer in the United States Marine Corps from 1978 thru 1986, and in the Reserve to the end of 1999, retiring after 22 years. He served as both an Infantry Officer and Intelligence Officer, in the US and on many overseas assignments, in war and in peace.

Larry was also a senior member of the Corporate Security Staff at BASF Corporation for over 16 years. During that time, he was the company's point man in managing sensitive chemicals, especially narcotics and weapons precursors. He has been a partner of DEA's Chemical Operations Division for many years, and has worked on several key counter-diversion projects over that time.

In July, Larry joined the DHS as their resident security expert on the chemical and petrochemical industries.



**Homeland
Security**

FOR OFFICIAL USE ONLY